

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT
Thurgood Marshall U.S. Courthouse 40 Foley Square, New York, NY 10007 Telephone: 212-857-8500

MOTION INFORMATION STATEMENT

Docket Number(s): 14-42 Caption [use short title] _____

Motion for: Leave of Court to File Amicus Brief ACLU v CLAPPER, ET ALL
and Attached Brief

Set forth below precise, complete statement of relief sought:

Movant is a primary witness in facts in the case and requests

the court allow him to file an Amicus Brief, and appear for Oral Argument as necessary.

Movant provided a previous motion which was not determined implicitly by the court.

Movant believes however the court considered his previously filed brief in this cause in oral arguments.

MOVING PARTY: John S. Stritzinger OPPOSING PARTY: American Civil Liberties Union

☐ Plaintiff ☒ Defendant
☐ Appellant/Petitioner ☐ Appellee/Respondent

MOVING ATTORNEY: Pro-SE OPPOSING ATTORNEY: Alexander Abdo
[name of attorney, with firm, address, phone number and e-mail]

John S. Stritzinger
PO BOX 1029
MEDIA, PA 19063

Court-Judge/Agency appealed from: (See Stritzinger v Verizon - 14-50090 - US Fifth Circuit)

Please check appropriate boxes:

Has movant notified opposing counsel (required by Local Rule 27.1):
☒ Yes ☐ No (explain): _____

Opposing counsel's position on motion:
☐ Unopposed ☐ Opposed ☒ Don't Know

Does opposing counsel intend to file a response:
☐ Yes ☐ No ☒ Don't Know

**FOR EMERGENCY MOTIONS, MOTIONS FOR STAYS AND
INJUNCTIONS PENDING APPEAL:**

Has request for relief been made below? ☒ Yes ☐ No

Has this relief been previously sought in this Court? ☐ Yes ☒ No

Requested return date and explanation of emergency: _____

Is oral argument on motion requested? ☒ Yes ☐ No (requests for oral argument will not necessarily be granted)

Has argument date of appeal been set? ☐ Yes ☐ No If yes, enter date: _____

Signature of Moving Attorney:
John S. Stritzinger (Pro-SE) Date: 08/24/2015

Service by: ☐ CM/ECF ☒ Other [Attach proof of service]

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT
NEW YORK, NY

CAUSE 14-42

ACLU v CLAPPER, ET ALL

DRAFT 3.7

Respondent's Brief in Regards to the 2nd Circuits Order to advise the court on the Status of the
Current Cause in relationship to Public Law 114-23

John S. Stritzinger

695 Bluff Pt

Columbia, SC 29212

jstritzinger3@yahoo.com

803.728.9238

MOTION FOR LEAVE OF COURT TO FILE AMICUS BRIEF

Respondent, John S. Stritzinger provided a previous Motion to this court, and the 9th Circuit to join the current cause and the related cause of (Smith v Obama) which was not explicitly determined. Petitioner believes the court did however review his issues presented.

Petitioner apologizes to the court for late filing but was not a recipient of specific orders in this cause. Petitioner hopes the court will consider the attached brief and the requested relief which he believes is in-line with the court's order. If he is accepted into the cause he will re-offer it as directed. Petitioner has provided his deposition to counsel in a related cause.

Petitioner informs the court he is litigating some of these issues in the SC under Sr. District Judge Wooten in the causes of Stritzinger v General Services Administration, et al, and Stritzinger v Travis County Texas, et al, and have previous orders in Stritzinger v Verizon (14-50090) in the Fifth Circuit.

Respondent is John S. Stritzinger

Signed This Day Electronically

08/20/15

A. ISSUES FOR REVIEW

ISSUE #1 – JURISDICTION & RELATED ITEMS WITH NATIONAL SECURITY POLICY

ISSUE #1A – JURISDICTION OF THIS COURT IN THE CURRENT PROCEEDING

ISSUE #1B – PRESIDENTS AUTHORIZATION OF VERIZON TO BUILD AN EXTENDED METADATA SYSTEM FOR THE US GOVERNMENT IN JUNE OF 2013.

ISSUE #1C – US SUPREME COURT RULES – MANDATES ISSUED IN THE NAME OF THE PRESIDENT OF THE UNITED STATES.

ISSUE #1D – CONGRESSIONAL APPROVAL OF THE PRESIDENTS POLICY ON METADATA.

ISSUE #2 – SCOPE OF THE DISCUSSION ON METADATA, ENHANCED LOCATION RECORDS, AND OTHER CPNI

ISSUE #3 – OWNERS, AND EXTENT OF METADATA, AND "ENHANCED METADATA".

ISSUE #4 – COMMERCIAL USES OF ENHANCED METADATA FOR RESIDENTIAL, ENTERPRISE, AND GOVERNMENTAL PURPOSES

ISSUE #5 – NECESSITY AND CONSTITUTIONALITY OF THE PATRIOT ACT, AND RELATED ACTS

ISSUE #6 – IS USE OF PRIVATE PUBLIC TRADED COMPANIES TO EXTEND US NATIONAL SECURITY POLICY ILLEGAL?

ISSUE #7 – CAN INFORMATION SERVICES PROVIDERS UNDER THE TELECOMMUNICATION ACT, PRIVATE BUSINESSES, AND MUNICIPALITIES STORE EXTENDED METADATA ON THEIR CUSTOMERS AND FOR WHAT DURATION?

ISSUE #8 – NEW HOME FOR DOMESTIC NSA PROGRAMS, A COMMON US REPOSITORY FOR EXTENDED METADATA.

ISSUE #9 – RELATED CAUSES AND IMPACT TO SCOPE OF SEARCH AND USES OF EXTENDED METADATA.

B. PARTIES

ACLU via its Primary Counsel

Represented By

Jameel Jaffer
American Civil Liberties Union Foundation (nyc)
[contact info](#)

Alexander Abraham Abdo
American Civil Liberties Union, Women'S Rights Proj
[contact info](#)

Brett Max Kaufman
American Civil Liberties Union
[contact info](#)

Catherine Newby Crump
American Civil Liberties Union Foundation (nyc)
[contact info](#)

Laura Donohue
Georgetown Law
[contact info](#)

Patrick Christopher Toomey
American Civil Liberties Union Foundation (nyc)
[contact info](#)

United States of America via its Primary Counsel

Represented By

Christopher Blake Harwood
United States Attorney'S Office
[contact info](#)

David Stuart Jones
[contact info](#)

Tara Marie La Morte
U.S. Attorney'S Office, Sdny (chambers Street)
contact info

John Dalton Clopper
U.S. Attorney'S Office, Sdny
contact info

Verizon via its counsel of Record Mr. Alan Albright

111 Congress Avenue
Suite 2300
Austin, Texas
78701-4061
P: +1.512.494.3620
F: +1.512.479.3920
alan.albright@bgllp.com

Bank of America via its counsel Ms. Tara Tune

Norton Rose Fulbright

Austin
T:+1 512 536 5253
F:+1 512 536 4598
tara.tune@nortonrosefulbright.com

Other Parties as identified by the court.

C. TABLE OF CONTENTS

TABLE OF CONTENTS FORTHCOMING

D – CITATIONS

Klayman v Obama (Consolidated 15-4017 – Pending US Court of Appeals DC Circuit)

US v Jones - (US Supreme Court-2012)

Riley v California (US Supreme Court – 2014)

Stritzinger v Verizon (Fifth Circuit – 14-50090)

US v Knotts (US Supreme Court-1983)

US v Q. Davis (11th Circuit)

E – JURISDICTION

Petitioner believes this court only has jurisdiction over issues which are not included in Statute, over its opinion of the US District Court's injunction in the District of Columbia, and its opinion on the opportunities to use extended metadata systems in this court's operating Circuit.

F – STATUTES

Fourth Amendment to the US Constitution

Fifth Amendment to the US Constitution

Telecommunication Act of 1996

Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701–2712)

The **Selective Service Act** or **Selective Draft Act**(Pub.L. 65–12, 40 Stat. 76, enacted May 18, 1917)

G – FACTS

The President of the United States authorized Verizon to build a real-time and ubiquitous enhanced location, and metadata storage system in June of 2013, prior to the US District Court's Trial in Klayman v Obama. Verizon has an existing program impacting its own customers (More than 100M), and has the capability to manage the other estimated 200M devices on US Soil. The Global population of devices of which Verizon is an International Telecommunications provider is approximately 3 Billion Devices according to Oracle, and likely approaching 10B in the next decade. This was an offshoot to an NSTAC program begun in 2008 by many participants. Thereafter the US District Court entered an injunction against the US Government from procuring or using the same. Verizon has not offered whether they want to accept this contract which is still under review.

Work on extended metadata systems began in a Federal context out of a Presidential program developed by the Bush, and Obama administrations called NSTAC which includes two presidential Executive Orders 12382 and 12472 and began in classified and non-classified work streams in a time of war. Furthermore many companies have developed GPS based systems as early as 1983 (See US v Knotts – US Supreme Court) and have related technologies (See AEGIS, AWACS) etc.

Respondent believes that due to the Patriot Act (PL-107), and HR2048 (PL-114), US Supreme Court Rules, and Article III of the US Constitution (As the President is certainly an ambassador) that the US District Court in the District of Columbia exceeded its authority by entering an injunction against the President and his national security team of which Respondent was an unpaid advisor, but has requested he be compensated out of HR2048 – Section 106. Furthermore, the 11th Circuit Court of Appeals (See US v Q. Davis) has overturned the injunction he believes on its own in a recent en-banc ruling which allows extended metadata systems to be used for criminal investigations.

Respondent believes this court's review of bulk collection of metadata to be only useful in the context of the ownership of the metadata repository, the uses of the metadata, and the duration of the record store which has not been decided by any US Court. All other issues Respondent believes are the responsibility of the US Supreme Court which has already decided these issues in US v Jones (2012), US v Knotts (1983), and Riley v California (2014). Respondent believes the ACLU only has a case if it can prove that it has been harmed by the collection of metadata which it cannot do without specific examples of harm, as the request is going against the rest of the Federal code base in regards to national security. Respondent however was harmed, when he believes the FBI, and the Whitehouse were insulted that Verizon did not offer commercial terms to them immediately, and actually placed him on an FBI watchlist which included counter-terror enforcement. Respondent believes the parties involved in signing a national security order against himself should be court-martialed as he was instructed that NSTAC members as published on the FBI website carried a US Military equivalent of a Three Star General. In other words the FBI sought to enforce against its own team when they thought the program was in jeopardy. Alternatively, Respondent may have been subjected to State Courts such as Virginia or Texas who believe via Capias Warrants have all the same powers in a State Context that the Federal Government does via its own Federal Code.

(<http://www.uscourts.gov/statistics-reports/wiretap-report-2012>). Respondent also recognizes that Verizon, Bank of America, and HP via their own legal teams including Wilmer Hale often in his opinion hire their own investigative teams which are on par or exceed FBI investigative resources which are limited and may have contributed to his situation.

Respondent was a member of the BAML Global Technology team which was asked/forced to participate in this program under TARP in Circa 2008/2009 by the Obama Administration. Respondent thereafter went to work for Civil Accounts at Verizon Federal where the issue of enhanced mobile security was requested by the Administration. Respondent believed this was a classified order under the Selective Services Act for a specific set of programs involving network

communications and security. Respondent believes the acts and omissions of the US Government are US National liabilities, and also its intellectual property in part, and via an acquisition of the same for 200M dollars from Verizon in whole. Related properties owned by BAML network services and the Hewlett Packard Corporation and their relationship to the materials acquired by the government are currently under review by the US Court of Appeals for the Fifth Circuit (See Stritzinger v Verizon, et ALL), and the SC US District Court in Columbia, SC. These issues have not reached the US Court of Appeals for the Fourth Circuit.

Respondent completed the work requested by the Administration and filed this information with the GSA, and Ms. Ruemeller of the White House Legal Staff at the request of the US Secret Service, and the Treasury Department.

There are multiple uses for extended metadata systems in the Federal Context which involve enforcing most of the Federal Code including counter-terror missions, building security, transportation security, border control, and employee safety, protective services and financial transaction verification. There are many more in residential, leisure and enterprise business uses. Respondent has in fact documented over 100 applications using the technology he developed on his own, with BAML, at Verizon and at the request of the US Government whose ownership needs to be determined. Some of these are classified, others sealed for further discussion. At the present time, Respondent believes he is the copyright holder in whole or in part for all such applications, and their related supporting architectures. This does not mean that other third parties might have a right to develop competing products, but he does believe that likely his own patents, and those with Verizon will play a part in most if not all of future solutions in these areas. Respondent has estimated the valuation of these items between 200M dollars and 50B dollars depending on how they are deployed in the global marketplace. This is a small fraction obviously of the US National Security budget.

OTHER – SPECIFIC COMMENTS TO THE CIRCUIT COURT'S OPINION

In a Previous Roles as a Senior Operations Manager of an International Telecommunications carrier, my Company had made use of a Call Detail Record Collection System (which we called CDR Query) which essentially archived every call made in the system using a standard billing format. It included a search engine which allowed us to troubleshoot customer problems on a maintenance event. For example, "My name is John Stritzinger, and I am having static on my line, and calls not completing to XXX-XXX-XXXX". Our process would simply to find the calls, and trunk groups in question, review failure codes, and identify any potential resolutions. This tool is common, and Verizon, ATT, and other Wholesale providers we worked with had one too. Our internal archive was typically set for thirty to Sixty Days depending on the customer, but could be extended on a Trunk Group or BTN for longer periods. IE if we had a specific need we could collect every call forever. We also could record calls if we received specific court orders which would include the call records, and the data itself. On a specific search warrant such as "US v Jones", this would be very straightforward.

In a mobile context, we have a similar challenge. We have customers who use our networks, and generate traffic both MMS, voice calls, data, and application services of all kinds. This same data is typically archived including location records on the switch, or a third party repository for 30-60 days, but like with call records can be extended.

While working at Verizon we developed a design to archive this material in real-time and for any length of time. In other words, if you take your cell phone into your bedroom, we essentially would know that at X:30 PM on August 23rd, your phone was at LATITUDE X, LONGITUDE Y, AND ALTITUDE Z. If this information is equated to a database which includes Geolocation data, in fact you can pinpoint exactly where any object is at any time. Furthermore, Cell phones have a handshake with the Cellular switch and via GSM/TDM protocols continue this is a persistent manner. In other words, US Carriers, already do keep extended metadata information for presence purposes, they simply don't offer services other than travel items typically for purchase. IE My Apple Maps program, TomTom, or Google Maps do display some ability to use location for a specific purpose.

Corporations and their specific core location kit of their cell phones and mobile applications can also run enhanced location databases which are unknown to the typical user. For example Chase might also store a copy of my LAT, LONG, and ALTITUDE for 30 days, but Bank of America may not. The result, what consumers get and use is completely arbitrary, and discovery in a legal context is in doubt. And in fact your location data may be stored in multiple jurisdictions and impacted by multiple possible legal processes. Such an unknown is expensive and dangerous and we must in fact have a legal remedy.

What we are suggesting is that only common carriers offer these services, that "Location Data " use registered core TCP/UDP Ports", and that specific retention of that data is published by the provider who offers it. The challenge is the standard which Yahoo uses might be different than Apple's, Verizon's, or Google's. Respondent has published a standard to do so which I will soon share with a wider audience.

Respondent believes the court's discussion now in three causes, falls below the level of a controversy which needs its approval, and the use of a CDR Query tool is in fact part of the telecommunications framework that Mr. Klayman, and Ms. Smith use every day. Respondent therefore believes that stopping the bulk collection of metadata in every context would essentially make it impossible or difficult for use to serve our own customers and is in fact ridiculous.

Respondent believes however the court taking up the issue of whether secondary actions of performing a query led to harm are however more serious. In general however I believe that the lower court's opinion was in fact the correct one, and not a harm to US National Security.

Respondent's does not however that the intent is to "colorize" or create VPN's for cellular objects which might include an FBI watchlist. So for example a Color Orange VPN would include all FBI subjects which need extended metadata solutions including call detail records, extended

location attributes, and computer forensics data on any increment, and interval and in near-real time. Respondent intends to make this data available to investigating agencies in real-time for a fee (and with full privacy) via automated interfaces which should eliminate the need for manual search warrants served to US carriers at tremendous costs, and with questionable recovery options. The standard would in fact be US v Jones requiring a Federal Court (and not a state Court) to issue an extended metadata solution.

Respondent argues that a State District Court – should be assigned a Federal peer for any requests its needs to carry out its duties and in fact the Federal Government should manage it. I think however that most State Supreme Courts might differ and so it likely would be the US Court's of Appeals, the Supreme Court, and Each State Supreme Court. At the end of the day, however, because of HR2048, and the Patriot Act, a US District Judge or FISA judge does have the power to deprive every right as a US Citizen, or Immigrant, and extended metadata systems make it easier to use. I think in the future however due to the presence of extended metadata in pervasive amounts from security and traffic cameras plus our own GPS enabled phones, we might be arguing about leniency of sentences and guidelines as a secondary review of metadata more often than not.

There are many interesting uses of Metadata systems which will automate everyday tasks such as sending me an instant message when the postman has just visited my home. This is the kind of automation which I think we all will appreciate, and are not in fact violations of our rights. Without extended metadata systems our lives would be much different. In other words not every extended metadata solution causes harm to the consumer, and a blanket request to remove them on its face sounds good but in fact a poor decision on multiple grounds. I think in time the ACLU will see that this is in fact true.

In the meantime if a court made an error in any party's handling of search, I think under the Constitution they have a right to complain and request damages. I just don't think in this particular case that argument is going to be sufficient.

My only advice to the consumer is to remember the simple fact that it should pretend that your cell phone is constantly in a court of law providing testimony to the court, and that literally any piece of data in any domain that it creates is theoretically discoverable. This includes Google, Apple, and Microsoft Domains, personal computers, and mobile devices. In fact HR2048, and the Patriot Act confirm. Our ability to provide national security is essentially our ability to provide these tools in as efficient manner as is possible. I believe Verizon is now the world leader in these areas, as is the financial services industry as a whole.

I advise the court to compel the required records to see if Mr. Klayman, Ms. Smith, and even myself have been impacted by a secondary search and enforcement efforts. If not the causes should be dismissed. If Mr. Klayman or his clients, or Ms. Smith had been impacted by a State Judge it seems to me that it would be difficult to tell. Its also not clear what enforcement options are available to parties who have received a material financial judgment. For example if

someone has a LIEN against my car, can he in fact install a GPS tracking device on my property. I think these are very interesting issues for the court to decide which would make this process useful.

In general however, I know that Mr. Klayman's lawsuit has caused us immense damage, and he should be concerned about his own liberty when he accuses the President of the United States of an impeachable crime. Myself, I know I have been physically harmed, and I merely want the FBI to tell me who did it. Once I understand that I believe I will be able to proceed in an orderly manner. We cannot however immediately shut down every request by individuals for damages solely on a national security grounds.

I believe for a lawsuit like this to occur, a show cause in a State or US District court reviewing one's harm should proceed first, before anything else is argued, as I am pretty confident that metadata, extended metadata, and computer forensics records will both now and the future be used for all types of purposes in every legal jurisdiction in the world. What will be different is the use of evidence, the retention policies, and the legal remedies.

I think the ACLU has however brought forward an interesting argument, and should be paid for their time dollar for dollar, but should not be awarded damages. I think the future, the court should have a specific show cause process for any related causes to extended metadata because an unknown legal barrier to entry will stop investment, and prevent innovative programs from hitting the market including medical, residential, and leisure programs which are in fact the most exciting programs ever in our history, and are in fact the future of our industry. As it turns out the US will likely be the global leader in these technologies if the US District Court Junction in DC is overturned explicitly.

H - ARGUMENTS

ISSUE #1 – JURISDICTION & RELATED ITEMS WITH NATIONAL SECURITY POLICY

ISSUE #1A – JURISDICTION OF THIS COURT IN THE CURRENT PROCEEDING

Respondent believes this court owns jurisdiction to the uses of extended metadata for federal enforcement for real-time applications, as discussed previously subject to an injunction entered by the US District Court in DC (Leon) which he believes needs to be overturned. For example there are less than 40K FBI employees, yet more than 1M parties on the FBI's watchlist (See FBI.GOV). Respondent believes without extended metadata systems inclusive of location records, that the US Government cannot perform its mission. This is a moot point however with the passage of the Patriot Act and its Ammendment HR2048.

ISSUE #1B – PRESIDENTS AUTHORIZATION OF VERIZON TO BUILD AN EXTENDED METADATA SYSTEM FOR THE US GOVERNMENT IN JUNE OF 2013.

The President's authorization of Verizon to build an enhanced metadata system is not an issue this court has authority over due to Article III of the Constitution which reserves this right to the US Supreme Court.

ISSUE #1C – US SUPREME COURT RULES – MANDATES ISSUED IN THE NAME OF THE PRESIDENT OF THE UNITED STATES.

The Supreme Court issues orders in the Name of the President of the United States, as such the President's own orders by the Supreme Court's own rules are equal in power. Respondent believes that a US District Court cannot under its own power restrain the president in any manner which is enforceable under US Code without an impeachment process. In this case, the ACLU cannot prove the same.

Ms. Smith (See Smith v Obama – 9th Circuit) may actually be able to prove harm IF and only if she can show that 1) she was targeted with collection 2) the collection lead to extended law enforcement actions 3) she was harmed by the same. The ACLU by issuing a collective claim without the same cannot and this cause should be dismissed. Mr. Klayman, and parties associated and enjoined with his cause are also claiming harm, which I believe need to follow the same tests. If not, I believe he should be labeled a vexatious litigant, the cause dismissed, and him sanctioned for exposing US National Security policy to the US Court System.

ISSUE #1D – CONGRESSIONAL APPROVAL OF THE PRESIDENTS POLICY ON METADATA.

Respondent believes that even if this court believes the President's authority is not governed under Article III, which it may, Respondent believes that Congress has given that power to the President explicitly. This court however should discuss the commercial uses of extended metadata systems, record stores, and the management of the same in context of the ACLU's complaint. Respondent believes however that a specific Search Warrant as seen in US v Jones would be required even if the US had a single US repository for metadata or 64 Copies (Each US State, 12 US Courts of Appeals, District of Columbia, Guam, Puerto Rico).

ISSUE #2 – SCOPE OF THE DISCUSSION ON METADATA, ENHANCED LOCATION RECORDS, AND OTHER CPNI

Respondent believes the current definition of extended metadata systems has been modified by the US Congress in HR2048. Respondent has offered his own definition which actually includes computer forensics.

ISSUE #3 – OWNERS, AND EXTENT OF METADATA, AND "ENHANCED METADATA".

Respondent believes that a non-investigative agency such as NASA, US Courts, or the Whitehouse legal staff should own the US repository and not the NSA, FBI, Treasury or other investigating agency.

ISSUE #4 – COMMERCIAL USES OF ENHANCED METADATA FOR RESIDENTIAL, ENTERPRISE, AND GOVERNMENTAL PURPOSES

Respondent notifies the court that the ACLUs goal to eliminate metadata storage was already decided by US v Knotts, US v Jones, and Riley v California, along with the 11th Circuit Ruling in US v Q. Davis. Respondent believes the ACLU complaint is devoid of merit or any other individuals who can claim specific harm.

ISSUE #5 – NECESSITY AND CONSTITUTIONALITY OF THE PATRIOT ACT, AND RELATED ACTS

Respondent believes that this court's own Mandate, US v Knotts, US v Jones, Riley v California, and US v Q. Davis on their own are sufficient to run a National Security Program unfettered and that the Patriot Act, and HR2048 should be struck in their entirety as unconstitutional. In effect we have given the power of officials in the Government to deprive all life, liberty, and freedom from US Citizens and foreign nationals without due process of Law. Respondent however would argue that on a 5th Amendment ground and not the 4th Amendment claim the ACLU has used. Respondent believes that all National Security order requests via the NSA or FISA judges should have specific defense council appointed for the party in question prior to any order being signed. There is no such provision of the Patriot Act or HR2048. In other words any US Federal agent can authorize another US citizen to be virtually killed by the Federal Enforcement divisions. Respondent believes that this in fact has happened to him for voicing opposition to the President Using US companies rather than Federal Employees to enforce Federal Laws.

In fact the FBI was asking NSTAC companies to respond to counter-terror threats with their own employees, and contractors during a time of war. Respondent does not know if this is still occurring. The result is that NSTAC companies, and the FBI were responding to threats in the 2nd Circuit's jurisdiction in any matter they deemed fit, which is probably unknown to the US public. Respondent believes that this was a force multiplier for the FBI for which they should be paid. Furthermore, Respondent has estimate the liability the US government has transferred to its member institutions to be in the Trillions of Dollars.

Respondent believes in effect other than the US Domestic Debt, the US Government has actually incurred liabilities which far exceed what has been published. If the US Court's absolve US Companies claims in the same that is fine, but My family and I for example, and all employees involved in NSTAC programs at BAML might actually be due hundreds of millions of dollars in damages, changes in names, and social security numbers as seen in the Federal Witness Protection programs.

ISSUE #6 – IS USE OF PRIVATE PUBLIC TRADED COMPANIES TO EXTEND US NATIONAL SECURITY POLICY ILLEGAL?

Respondent believes that the President without signing a specific Executive Order, must seek Congress to modify its Selective Services Act to incorporate special circumstances. Respondent believes verbal orders of the President should carry the same weight, and therefore the president has not broken the law, unless he retracts the same.

Respondent believes that if the President does not honor his commitment to NSTAC companies, and Verizon that he in fact did break the law, citing multiple breaches of the US Selective Services act for each and every individual and company participating in NSTAC which I believe he is guilty. This liability should extend back to Mr. Bush's presidency when he signed the law initially. Respondent believes that Federal Contractor's seeking Federal Business did not have the opportunity to decline for literal fear for their life under the Patriot Act, as did Respondent.

Respondent also takes objection to the US Justice Department continued to sue and seek regulation of the Financial Industry while at the same time generating liabilities beyond the companies ability to pay. On behalf of Bank of America, I believe that Bank of America should not pay a recent mortgage settlement as an offset against the classified orders entered by the US Government during TARP. This is greater than 10B dollars, and consumed a great deal of energy. Petitioner believes the government could instead invest more in the FBI so that it can manage its own watchlist via its own staff at a ratio of 1:2 or less. In other words, the FBI would likely need upwards of 500K people to manage 1M people on the US watchlist.

ISSUE #7 – CAN INFORMATION SERVICES PROVIDERS UNDER THE TELECOMMUNICATION ACT, PRIVATE BUSINESSES, AND MUNICIPALITIES STORE EXTENDED METADATA ON THEIR CUSTOMERS AND FOR WHAT DURATION?

Petitioner believes that only licensed regulated carriers under the Telecommunications Act of 1996 should be able to own and operate metadata storage. For example Bank of America should not be able to keep and own metadata but should have to purchase it from the licensed carriers who offer this service such as LNP services using a reciprocal compensation model. This will protect US Carriers who have to invest in these systems.

ISSUE #8 – NEW HOME FOR DOMESTIC NSA PROGRAMS, A COMMON US REPOSITORY FOR EXTENDED METADATA.

Petitioner believes that the NSA's domestic programs should be moved to a Federal Contractor operating on its behalf. Petitioner believes Verizon has been hired for the same.

ISSUE #9 – RELATED CAUSES AND IMPACT TO SCOPE OF SEARCH AND USES OF EXTENDED METADATA.

As per this court's previous conversation on Seizure versus Search, the storage of extended-metadata services have in fact been authorized by the President and Congress. Search however is governed now by US v Jones. Petitioner with Verizon has developed copyright and soon patents on the use of radial Metadata court processes which return location records at a distance from a crime scene for a fee. (See US v Q. Davis)

RELIEF REQUESTED

- 1) Respondent requests that the court provide its input to the issues he offered for each of the items presented.
- 2) Respondent requests the court provide an order allowing for himself, Bank of America and Verizon to get paid under HR2048 Section 106 for our legal expenses, security, liabilities and time related to the matter.
- 3) Respondent requests the court order the ACLU, and other regulated FCC Telecommunications carriers to provide at least one cleared representative to review both classified and non-classified programs to prevent ongoing litigation around their use within 180 days or as coordinated by Verizon.
- 4) Respondent requests an order informing the GSA to provide the following:
 - a) Contract to Either Verizon or a Company run by respondent to manage extended metadata systems.
 - b) Order the SC District court to review payment for initial capital invested for extended metadata systems of 200M dollars, excluding services covered under GSA Network contract within ten days, if it has not already done so.
 - c) Order the NY District Court under the Honorable Judge Pauley to review extended metadata applications and their use in the 2nd Judicial Circuit after the SC District court completes its process under a closed process.
- 5) Respondent requests an order to Compel Bank of America, and the United States to produce for the parties in this cause any terms of the MOU representing respondent, electronic communications, and controls of employee relationships including NSTAC.
- 6) Respondent requesting the Government produce any enforcement information it has regarding Ms. Anna Smith (See Anna Smith v Barrack Obama), or the parties claiming harm in Klayman v Obama.
- 7) Respondent requests the court establish a process to review damages from parties harmed via NSTAC programs including his own family.

UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

CAPTION:

American Civil Liberties Union v.

PO BOX 1029

MEDIA, PA 19063

CERTIFICATE OF SERVICE

Docket Number: 14-42

I, John S. Stritzinger, hereby certify under penalty of perjury that on
(name)

_____, I served a copy of _____
(date)
Motion for Leave of Court, Amicus Brief

(list all documents)

by (select all applicable)*

- ☐ United States Mail
- ☒ Federal Express
- ☐ Overnight Mail
- ☐ Facsimile
- ☒ E-mail
- ☐ Hand delivery

on the following parties (complete all information and add additional pages as necessary):

<u>Alexander Abdo</u>	<u>Lead Counsel-ACLU</u>	<u>NY</u>	<u>NY</u>	
Name	Address	City	State	Zip Code
<u>A. Eisenberg</u>	<u>Counsel - ACLU</u>	<u>NY</u>	<u>NY</u>	
Name	Address	City	State	Zip Code
<u>D. Letter</u>	<u>Counsel - United States</u>	<u>NY</u>	<u>NY</u>	
Name	Address	City	State	Zip Code
<u>H. Whitaker</u>	<u>Counsel - United States</u>	<u>NY</u>	<u>NY</u>	
Name	Address	City	State	Zip Code

08/24/2015

Today's Date

ACLU v CLAPPER, ET ALL

Signature

*If different methods of service have been used on different parties, please indicate on a separate page, the type of service used for each respective party.